(12) UK Patent Application (19) GB (11) 2 197 734 (13) A

(43) Application published 25 May 1988

(21) Application No 8726373

(22) Date of filing 11 Nov 1987

(30) Priority data
(31) 8627253 (32) 14 Nov 1986 (33) GB

(71) Applicant
Louis Newmark PLC

(Incorporated in United Kingdom)

Newmark House, 143/149 Great Portland Street, London, W1N 6BP.

(72) Inventors
Bernard John Regan
Herbert Collomosse

(74) Agent and/or Address for Service
F J Cleveland & Company,
40-43 Chancery Lane, London, WC2A 1JQ.

(51) INT CL⁴
G06F 12/14

(52) Domestic classification (Edition J):
G4A AP

(56) Documents cited
GBA 2061578

(58) Field of search
G4A
G4H
Selected US specifications from IPC sub-class G06F

(54) Computer security system

(57) Apparatus for controlling access to a computer from peripheral equipment 11, such as a VDU terminal includes a first part such as a lock 12 which can be connected in the line between the equipment 11 and the computer 10 so that it normally isolates them . A second part e.g. a portable unit can be located, 15, relative to the first part such that it can transmit a code to the control unit of the first part. The control unit checks the code and opens the line if a valid code is sensed. The lock also includes means permitting input from terminal 11 to the control unit of a character or characters relating to a password and the control unit is arranged on the basis of the input characters to generate according to a stored procedure a password for transmission to the computer.

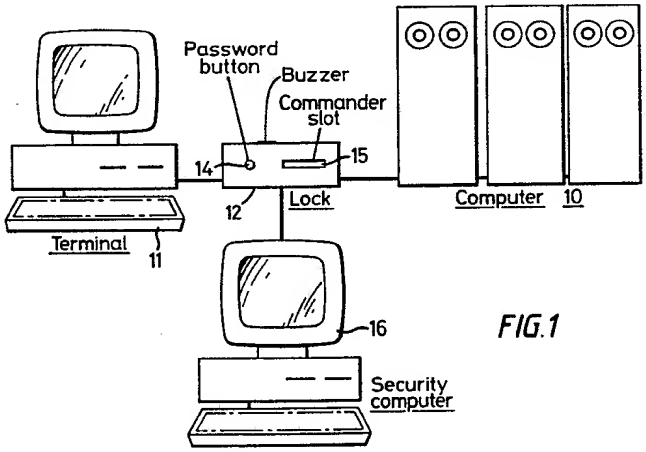

FIG.1

GB 2 197 734 A

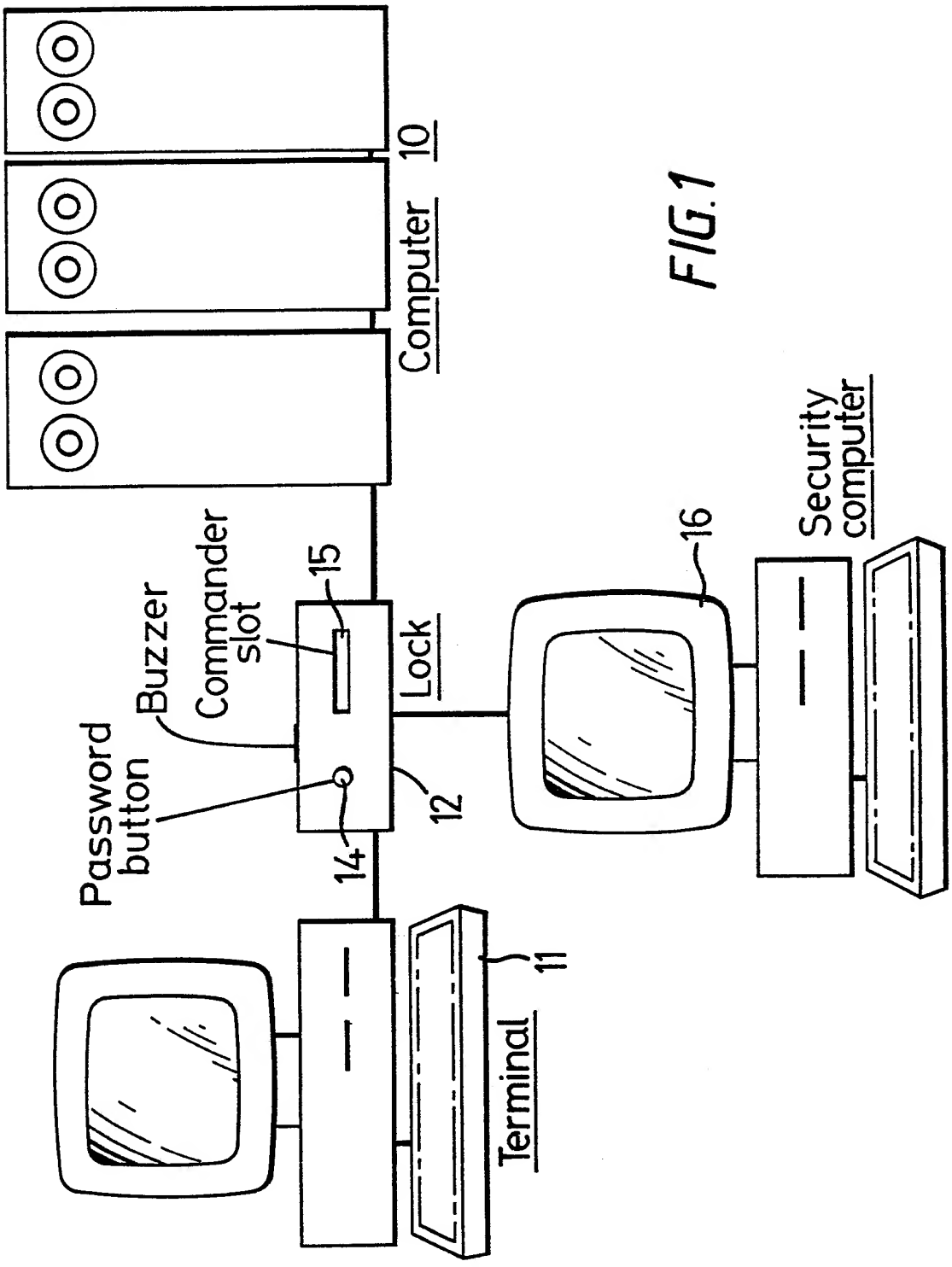
Computer 10
Commander slot
15
Buzzer
Password button
Lock
12
14
16
Security computer
Terminal 11

FIG.1

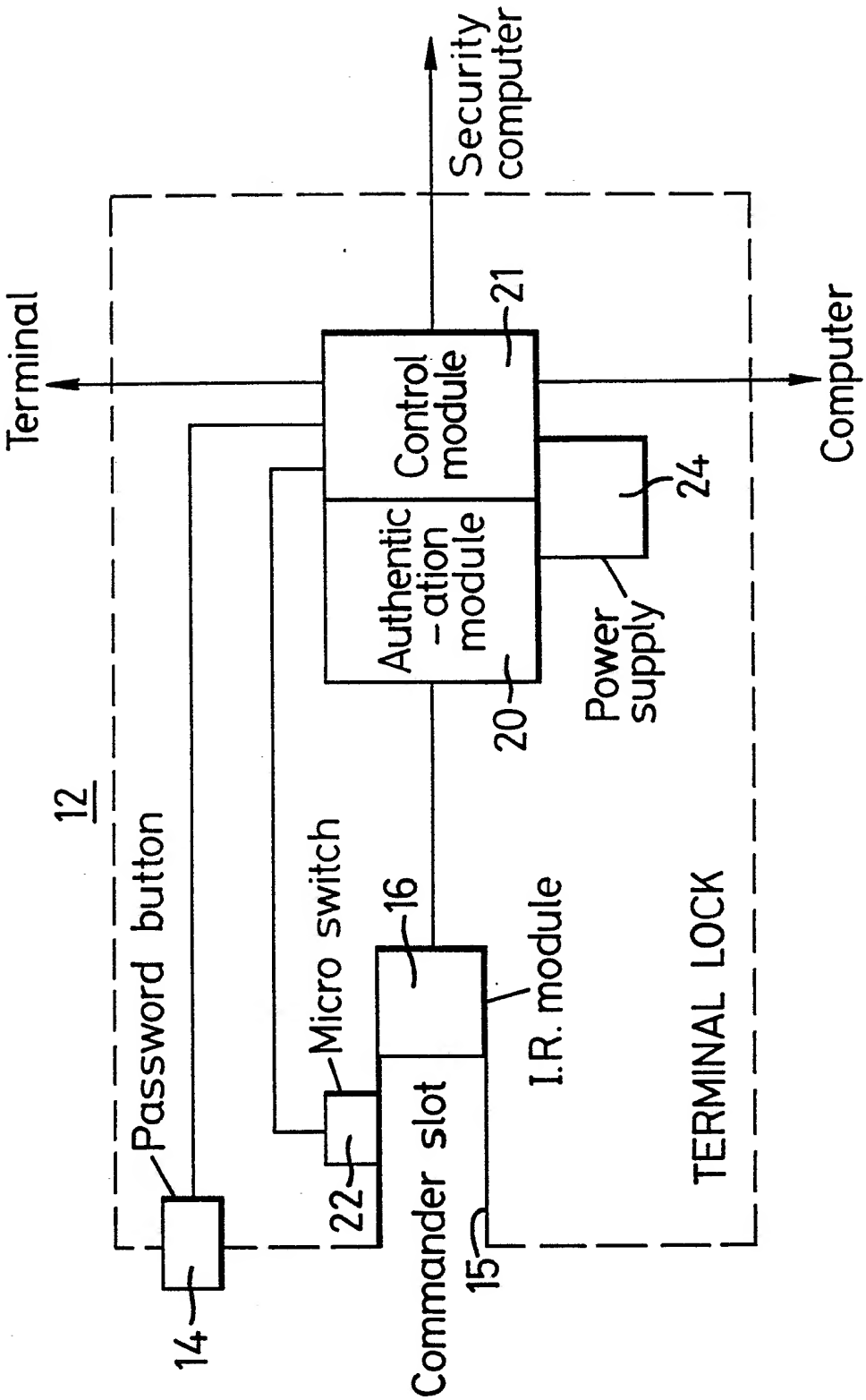

FIG. 2 Terminal lock block diagram.

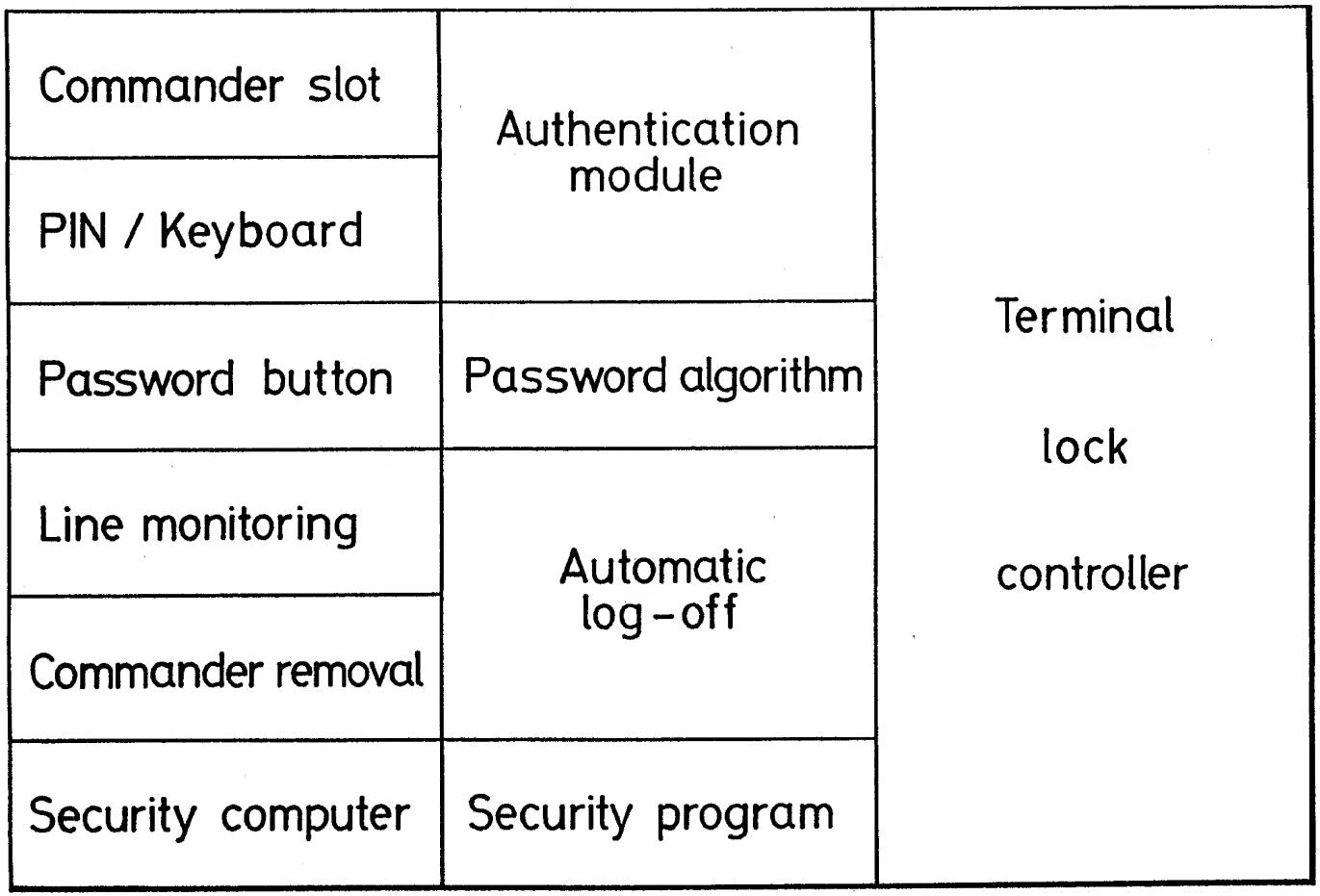

FIG.3 Terminal lock functional diagram.

2107734

COMPUTER SECURITY SYSTEM

This invention relates to the security of computer systems.

It is well known in computer systems to require the entry of the password or passwords in order to gain access to the system accounts. This type of arrangement provides only a relatively low level of security since the passwords tend to become known and can in some cases be evaded. The present invention is concerned with apparatus which is designed to provide an improved level of security.

According to one aspect of the present invention there is provided apparatus for controlling access to a computer from peripheral equipment such as a VDU terminal, said apparatus including a first part which is arranged to be connected in the line between the equipment and the computer so that it normally isolates said equipment and computer, and a second part which can be located relative to the said first

part such that it can communicate with the control unit of said first part, said second part being arranged to transmit to the control unit a code and said control unit being arranged to check the validity of said code and to open said line if a valid code is sensed, said first part also including means permitting input to said control unit of a character or characters relating to a password and said control unit being arranged on the basis of the input characters to generate according to a stored procedure a password for transmission to the computer. The communication between the second part and the control unit can be a two way communication.

The apparatus may be arranged to transmit the password to the computer only if that password is recognised as one validly associated with the code transmitted by the second part.

The entry of said character or characters may result in the production of two elements of the password which are manipulated by the control unit in accordance with an algorithm to produce the password.

This arrangement has the advantage that the passwords used in the system need never become known to the user. What a user does is input characters which select a particular system account and on the basis of those characters the control unit generates the appropriate password which is only transmitted to the computer if it is recognised as one validly associated with that user.

The second part may be a hand held unit insertable by by any user into a receiving slot or the like in the first part to permit communication with said control unit. The communication may be by way of an infra-red link, a radio type link, a magnetic type link or any other suitable means. The control unit may be arranged to check both that said second part is an authorised device and that the code transmitted to it is an authorised code.

The apparatus may include a facility for disabling a line between the peripheral equipment and the computer subsequent to that line having been opened in response to the generation of a valid password. This facility may be operable when said control unit senses a predetermined period of inactivity on said

line, when said control unit senses that said second part is no longer operationally coupled to the first part but said peripheral equipment is not logged off, or when said control unit senses that said peripheral equipment has been logged off but said second part is still operationally coupled to the control unit.

According to another aspect of the present invention there is provided apparatus for controlling access to a computer from a peripheral equipment such as a VDU terminal, said apparatus including a first part which is arranged to be connected in the line between the equipment and the computer so that it normally isolates said equipment and computer, and the second part which can be located relative to said first part so that it can communicate with a control unit of said first part, said second part being arranged to transmit to the control unit a code and said control unit being arranged to check the validity of said code to open said line if a valid code is sensed, and wherein said second part includes a facility for disabling the line between the peripheral equipment and computer subsequent to that line having been opened. The communication between the second part and the control unit can be a two way communication.

Said facility may be operable when said control unit senses a predetermined period of inactivity on said line, when said control unit senses that said second part is no longer operationally coupled to said control unit but that said peripheral equipment is not logged off, or when said control unit senses that said peripheral equipment has been logged off and that said second part is still operationally coupled to the control unit.

The invention will be described now by way of example only with particular reference to the accompanying drawings. In the drawings:

Figure 1 is a block schematic diagram of a computer system incorporating security apparatus in accordance with the present invention;

Figure 2 is a block schematic diagram of a security apparatus in accordance with the present invention, and

Figure 3 is a block diagram illustrating the function of the apparatus.

Referring to Figure 1 a computer system comprises a main computer illustrated at 10, a terminal 11, and security apparatus hereinafter referred to as a lock 12 which is connected in the line between the terminal 11 and computer 10. The lock 12 has a button 14 whose function will be referred to later. The lock 12 also has a slot 15 which can receive a small hand held unit which will hereinafter be referred to as a commander.

The commander can communicate with circuitry in the lock 12 by any suitable means. In the present embodiment the communication is by means of an infra-red link but it will be appreciated that other types of arrangement could be used such as magnetic cards or radio tags. The lock 12 also incorporates a buzzer which acts as an alarm as will be decribed hereinafter. Also shown on Figure 1 is a security computer 16.

Referring now to Figure 2 the lock is a processor based device and includes an authenication module 20 and a control module 21 both of which are micro-processor based devices. The commander slot is shown at 15 and is terminated by an infra-red module 16 which is connected to the authentication module

20. The button 14 is connected to the control module which itself has connections both to the terminal 11 and to the computer 10. It also has a connection to the security computer 16. A micro switch 22 is provided adjacent the slot 15 and is connected to the control module 21. The unit includes a power supply 24 for supplying the necessary power to the authentication module and control module.

The function of the lock 12 in conjunction with a commander is to control access to the computer 10 from the terminal 11.

In use on power-up the lock 11 assumes a locked state in which the terminal 11 and computer 10 are isolated via the control module 21. A user wishing to access the computer 10 can only do so by making use of his commander unit. Initially the commander is inserted into the commander slot 15. In this position the commander can communicate with the authentication module 20 by way of the module 16. The authentication module initially carries out a check to ensure that the commander unit inserted is an authorised unit. Information regarding those commander units which are authorised is stored within

the authentication module 20 to enable it to carry out this function. In addition to using a valid commander the user has to enter via the terminal keyboard a personal identification number or code which is unique to that user. This number is communicated to the authentication module which checks that it is the number of an authorised user associated with that particular commander. The authentication module has previously been provided with that number as an authorised number. If the correct identification number is entered then the control module 21 is instructed to open the link between the terminal 11 and the computer 10 so that the user wishing to gain access can transmit characters from the terminal to the computer although cannot gain access to an account at that stage.

The user then has to enter a password in order to access an account of the the computer 10. The present arrangement does not make use of a conventional scheme for entering passwords. The password itself is not known to a user of the system. The system makes use of personal and system passwords. There can be a number of personal passwords and a number of system passwords. The user

initially operates the button 14 on the lock 12 and in response to this a message is displayed on the terminal 11 which prompts the user to select either a personal or system password. After selecting the type the user has to enter a number which in the case of a personal password will be a single character and in the case of a system password will be a two digit number. On entry of a valid password number a word known as a password tag is displayed on the terminal screen and the user is invited to either accept or reject this tag by pressing the return key. If the user accepts the tag then an algorithm stored within the control circuitry of the lock 12 generates a password for transmission to the computer 10. This password generation involves manipulation of a password seed and a password base. If the password is recognised as one which the user is entitled to use the user will be allowed access to the appropriate account within the computer. If not then access will be refused. Thus it will be seen that whilst the two elements required to generate a password may be known the actual password transmitted to the computer is not known and can be maintained completely secret.

During access to an account in the computer 10 the user is required to retain his commander in the slot 15. If the user removes his commander without logging off this is sensed by the control circuitry of the lock 12 and a message is displayed on the terminal 11 requesting replacement of the commander and the warning buzzer is also sounded. If the commander is not replaced within a given time which has previously been selected by the system manager the control circuitry of the lock 12 attempts to log the user off automatically. If this is successful the lock returns to its locked state so that the user can no longer access the computer 10. If automatic log-off is unsuccessful the lock alarm sounds for a programable time and sends a message to the security computer 16 to indicate that the automatic logoff has been unsuccessful. The users name and the commander number and the reason for the error condition are displayed on the terminal and repeated every ten seconds. The user must then replace his commander and complete the log-off procedure in order to remove this error condition. Alternatively a security officer may load a device in the slot 15 to correct the situation.

Automatic log-off is initiated by the control unit of the lock 12 transmitting a log-off command to the computer 10. The control unit then awaits a response from the computer following which it generates a further signal or signals to complete the log-off.

If the user replaces his commander in response to the warning referred to above he can again gain access to the computer by operating his commander and inserting his identification number as in the manner described above.

The lock also incorporates other functions operable in connection with log-off. These are as follows. If the user removes his commander immediately after a valid log-off has been recognised by the lock the lock checks that the user has logged off correctly. If the lock identifies a correct logoff then it assumes the condition in which the new user can gain access to the system in the manner described above. If the log-off is found to be incomplete, an automatic log-off procedure will be attempted in the manner described above.

If a valid log-off command is detected by the lock and this is followed by a pre-selected period of inactivity a short warning tone is generated. If following this the user does not enter any further information within a time specified by the system manager the lock carries out a check to see whether the user has logged off. If this is not the case the lock will attempt automatic logoff in the manner described above. If however, the user has already logged off an alarm is sounded and a message produced to indicate that the user has logged off but left the commander in the slot 15. When the commander is removed the alarm is cancelled and the lock assumes a condition in which it is ready to receive the next user.

If whilst logged on in the manner described above the lock detects a long period of inactivity on the line between the terminal and the main computer the user is requested to activate his commander and enter his identification number. If this operation is performed correctly the link between the terminal 11 and the computer 10 is maintained so that the user may continue interaction with the computer. If however the commander is not operated or an incorrect

identification number is entered the lock again attempts to logoff the user. If this is unsuccessful an alarm condition occurs. If however the log-off is successful an alarm is sounded to indicate that the user has left the commander in the slot 15. Again removal of the commander will cancel the alarm so that the lock again assumes a state in which it is ready to receive the next commander. Timing of automatic log-off is controlled by a system of timeouts which can configured to suit each particular installation.

It will be appreciated that generation of system passwords and information relating to valid commanders will be under the control of a security manager. The security manager can enter data relevant to these parameters into the authentication and control modules 20,21 using a special device known as a loader. Thus at any time the security manager can introduce details of a newly authorised commander or can delete details of a commander which is no longer to be used. Instead of using the loader it is possible to use an arrangement in which the security manager configures the system from a remote location.

It will be appreciated that the system software incorporates a plurality of timeout for example to control the timing of automatic log-offs. These timecuts are user configurable.

An important feature of the present system is the password facility. In the present embodiment up to 16 system passwords may be defined. A list of the passwords accessible to each user is entered when a new commander is introduced and may be edited by selecting a number from a main menu. Each system password has its own tag and is derived from its own base and the system seed. The tag is a string of characters which are displayed after the number of the password has been chosen by the user as a final check that this is the account required. For example a tag for a password used to gain entry to a mailing list may be MAIL LIST. The base is also a string of characters. When the password has been chosen and the tag determined to be correct the base is combined with the system seed and the resulting password sent to the main computer as described above. The system seed is also a string of characters and these can be set to a number of different characters values to give more distinct passwords. By changing the

password seed the security manager can simultaneously changes all system passwords. The lock allows passwords to be generated from the previous seed facilitating the mechanism of changing passwords.

User passwords are derived in a similar manner up to 4 for each user. Each user password has its own tag and base, each user has his own seed.

As a further feature which will provide an added level of security a plug in encryption unit can be provided between the terminal and computer.

CLAIMS:

1. Apparatus for controlling access to a computer from peripheral equipment such as a VDU terminal, said apparatus including a first part which is arranged to be connected in the line between the equipment and the computer so that it normally isolates said equipment and computer, and a second part which can be located relative to the said first part such that it can communicate with the control unit of said first part, said second part being arranged to transmit to the control unit a code and said control unit being arranged to check the validity of said code and to open said line if a valid code is sensed, said first part also including means permitting input to said control unit of a character or characters relating to a password and said control unit being arranged on the basis of the input characters to generate according to a stored procedure a password for transmission to the computer.

2. Apparatus as claimed in claim 1, wherein the communication between the second part and the control unit is a two way communication.

3. Apparatus as claimed in claim 1 or claim 2, wherein the apparatus is arranged to transmit the password to the computer only if that password is recognised as one validly associated with the code transmitted by the second part.

4. Apparatus as claimed in any preceding claim, wherein the entry of said character or characters results in the production of two elements of the password which are manipulated by the control unit in accordance with an algorithm to produce the password.

5. Apparatus as claimed in any preceding claim, wherein the second part is a hand held unit insertable by by any user into a receiving slot or the like in the first part to permit communication with said control unit.

6. Apparatus as claimed in any preceding claim, wherein the communication is by way of an infra-red link, or a a radio type link, or a magnetic type link.

7. Apparatus as claimed in any preceding claim, wherein the control unit is arranged to check both that said second part is an authorised device and that the code transmitted to it is an authorised code.

8. Apparatus as claimed in any preceding claim, including a facility for disabling a line between the peripheral equipment and the computer subsequent to that line having been opened in response to the generation of a valid password.

9. Apparatus for controlling access to a computer from a peripheral equipment such as a VDU terminal, said apparatus including a first part which is arranged to be connected in the line between the equipment and the computer so that it normally isolates said equipment and computer, and the second part which can be located relative to said first part so that it can communicate with a

control unit of said first part, said second part being arranged to transmit to the control unit a code and said control unit being arranged to check the validity of said code to open said line if a valid code is sensed, and wherein said second part includes a facility for disabling the line between the peripheral equipment and computer subsequent to that line having been opened.

10. Apparatus as claimed in claim 9, wherein the communication between the second part and the control unit is a two way communication.

11. Apparatus as claimed in claim 9 or claim 10, wherein said facility is operable when said control unit senses a predetermined period of inactivity on said line, when said control unit senses that said second part is no longer operationally coupled to said control unit but that said peripheral equipment is not logged off, or when said control unit senses that said peripheral equipment has been logged off and that said second part is still operationally coupled to the control unit.

12. Apparatus for controlling access to a computer substantially as hereinbefore described with reference to and as shown in the accompanying drawings.